The Divisibility of Some Divisibility Sequences

Universidad de Sevilla

December 14th, 2006

Co-workers

Manfred Einsiedler
Bríd Ní Fhlathuín
Helen King
Valéry Mahé
Gerry McLaren
Victor Miller
Ouamporn Phuksuwan
Jonathan Reynolds
Nelson Stephens
Shaun Stevens
Tom Ward

Two classical divisibility sequences:

(F) 1,1,2,3,5,8,13,21,34,55,89,144,...

Two classical divisibility sequences:

(F) 1,1,2,3,5,8,13,21,34,55,89,144,. . .

$$F_{n+2} = F_{n+1} + F_n$$

Two classical divisibility sequences:

(F) 1,1,2,3,5,8,13,21,34,55,89,144,. . .

$$F_{n+2} = F_{n+1} + F_n$$

(M) 1,3,7,15,31,63,127,255,. . .

Two classical divisibility sequences:

(F) 1,1,2,3,5,8,13,21,34,55,89,144,. . .

$$F_{n+2} = F_{n+1} + F_n$$

(M) 1,3,7,15,31,63,127,255,. . .

$$M_n = 2^n - 1$$

1. PRIME TERMS

Question

How many prime terms are there?

Probably both sequences have infinitely many prime terms.

Probably both sequences have infinitely many prime terms.

A proof seems beyond reach at the moment.

Probably both sequences have infinitely many prime terms.

A proof seems beyond reach at the moment.

However Mersenne and Fibonacci do produce primes in a less restrictive sense.

2. PRIMITIVE DIVISORS

Definition

A nonzero term B_n in an integral sequence $B = (B_n)$ has a **primitive divisor** $d > 1$ if:

(I) $d | B_n$

(II) gcd(B_m, d)=1 for all $m < n$ with $B_m \neq 0$.

All Fibonacci numbers have a primitive divisor after $F_{12} = 144$ (Carmichael 1914).

All Fibonacci numbers have a primitive divisor after $F_{12} = 144$ (Carmichael 1914).

All Mersenne numbers have a primitive divisor after $M_6 = 63$ (Bang 1886).

Primitive Divisors of Fibonacci

n	F_n	Factors of F_n
1	1	1
2	1	1
3	2	$\underline{2}$
4	3	$\underline{3}$
5	5	$\underline{5}$
6	8	2^3
7	13	$\underline{13}$
8	21	$3.\underline{7}$
9	34	$2.\underline{17}$
10	55	$5.\underline{11}$
11	89	$\underline{89}$
12	144	$2^4.3^2$
13	233	$\underline{233}$
14	377	$13.\underline{29}$

Bang's result applies to sequences of the form $a^n - 1, a > 1$.

Bang's result applies to sequences of the form $a^n - 1, a > 1$.

All terms after the 6th have a primitive divisor.

Bang's result applies to sequences of the form $a^n - 1, a > 1$.

All terms after the 6th have a primitive divisor.

The same result is true for sequences $a^n - b^n$ with $a > b > 0$ (Zsigmondy 1892).

Bang's result applies to sequences of the form $a^n - 1, a > 1$.

All terms after the 6th have a primitive divisor.

The same result is true for sequences $a^n - b^n$ with $a > b > 0$ (Zsigmondy 1892).

Remarkable: the bound 6 is

(a) uniform

Bang's result applies to sequences of the form $a^n - 1, a > 1$.

All terms after the 6th have a primitive divisor.

The same result is true for sequences $a^n - b^n$ with $a > b > 0$ (Zsigmondy 1892).

Remarkable: the bound 6 is

(a) uniform

(b) small.

Application - Group Theory

The order of some finite groups such as

$$\mathsf{GL}_n(\mathbb{F}_q)$$

where $q = p^r$, either as n or r grows.

Application - Group Theory

The order of some finite groups such as

$$\mathsf{GL}_n(\mathbb{F}_q)$$

where $q = p^r$, either as n or r grows.

Sylow's Theorem can be used to make predictions about subgroup structure.

A *Lucas sequence* $U = (U_n)$ is one given by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where α and β are conjugate quadratic integers. That is, roots of an irreducible quadratic polynomial $x^2 + Ax + B$ with $A, B \in \mathbb{Z}$.

A *Lucas sequence* $U = (U_n)$ is one given by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where α and β are conjugate quadratic integers. That is, roots of an irreducible quadratic polynomial $x^2 + Ax + B$ with $A, B \in \mathbb{Z}$.

Example The Fibonacci sequence is a Lucas sequence coming from $x^2 - x - 1$; where

$$\alpha = \frac{1 + \sqrt{5}}{2}, \beta = \frac{1 - \sqrt{5}}{2}.$$

Theorem

[Bilu+Hanrot+Voutier Crelle 2001] All the terms of a Lucas sequence U have a primitive divisor after U_{30}.

Theorem

[Bilu+Hanrot+Voutier Crelle 2001] All the terms of a Lucas sequence U have a primitive divisor after U_{30}.

This is a sharp result. The term U_{30} in the sequence coming from

$$\alpha = \frac{1+\sqrt{-7}}{2}, \beta = \frac{1-\sqrt{-7}}{2}$$

does not have a primitive divisor.

Factors of some U_n

n	U_n
6	5
10	-11
15	-89
30	$-24475 = -5^2.11.89$

Carmichael's paper from 1914 shows that all U_n have a primitive divisor after U_{12} when α and β are real.

Carmichael's paper from 1914 shows that all U_n have a primitive divisor after U_{12} when α and β are real.

The example of Fibonacci shows this is sharp.

Carmichael's paper from 1914 shows that all U_n have a primitive divisor after U_{12} when α and β are real.

The example of Fibonacci shows this is sharp.

General case requires very good bespoke estimates from Diophantine Approximation (Baker's Theorem) as well as a lot of computation.

Application - Diophantine Equations

Given $0 \neq D \in \mathbb{Z}$, BHV find all occasions when

$$x^2 + D = p^n$$

has more than one solution (x^2, p, n) with

$$x \in \mathbb{Z}, p \text{ a prime and } n > 1.$$

3. PERFECT POWERS

Look again at Fibonacci:

(F) $\underline{1}$,$\underline{1}$,2,3,5,$\underline{8}$,13,21,34,55,89,$\underline{144}$,...

Question

How many perfect powers are there?

Theorem[Bugeaud+Mignotte+Siksek Annals 2005] In the Fibonacci sequence, only the terms underlined are perfect powers.

Theorem[Bugeaud+Mignotte+Siksek Annals 2005] In the Fibonacci sequence, only the terms underlined are perfect powers.

Proof uses a deep combination of sharpened versions of classical transcendence results, 'modular' methods, as well as computational techniques.

Elliptic Divisibility Sequences

Let E denote an elliptic curve in Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6,$$

where $a_1, \ldots, a_6 \in \mathbb{Z}$ and $\Delta_E \neq 0$.

Let $P \in E(\mathbb{Q})$ denote a rational point on E. Write

$$x(P) = \frac{A_P}{B_P^2}$$

with $A_P, B_P(> 0) \in \mathbb{Z}$, in lowest terms.

Let

$$x(nP) = A_n/B_n^2.$$

Assuming P is non-torsion, the sequence

$$B = (B_n)$$

is called an **Elliptic Divisibility Sequence** (hereafter **EDS**).

Theorem(Silverman JNT 1988) There exists N_0 such that for all $n > N_0$, the term B_n has a primitive divisor.

Theorem(Silverman JNT 1988) There exists N_0 such that for all $n > N_0$, the term B_n has a primitive divisor.

Question What is the dependence of N_0 upon E and P?

Definition

Given any integer sequence $B = (B_n)$, if there is a greatest index n for which B_n has no primitive divisor, this index is called the **Zsigmondy Bound** and written $n = Z(B)$.

Definition

Given any integer sequence $B = (B_n)$, if there is a greatest index n for which B_n has no primitive divisor, this index is called the **Zsigmondy Bound** and written $n = Z(B)$.

Examples $Z(F) = 12$ and $Z(M) = 6$

Conjecture

If $B = (B_n)$ denotes an EDS coming from an elliptic curve in minimal form then $Z(B)$ is uniform, independent of E and P.

Conjecture

If $B = (B_n)$ denotes an EDS coming from an elliptic curve in minimal form then $Z(B)$ is uniform, independent of E and P.

This uniform bound might be 39.

Why minimal form?

If no assumption is made about E being in minimal form then arbitrary many denominators can be cleared and no uniformity result is possible.

Proof[Proof of Silverman's Theorem.]

The proof uses two important properties of an EDS (B_n).

(I) For odd primes p, if $p|B_n$ then

$$\mathrm{ord}_p(B_{np}) = \mathrm{ord}_p(B_n) + 1.$$

(When $p = 2$ you can get $+2$.)

Proof[Proof of Silverman's Theorem.]

The proof uses two important properties of an EDS (B_n).

(I) For odd primes p, if $p|B_n$ then

$$\mathrm{ord}_p(B_{np}) = \mathrm{ord}_p(B_n) + 1.$$

(When $p = 2$ you can get $+2$.)

(II) $\log B_n \sim hn^2$ for some $h > 0$ (B has quadratic exponential growth rate).

Step 1

Assume B_n does not have a primitive divisor. Given any $p|B_n$, if $p|B_m$ with $m < n$ then clearly

$$p|B_{\text{gcd}(n,m}$$

Step 1

Assume B_n does not have a primitive divisor. Given any $p|B_n$, if $p|B_m$ with $m < n$ then clearly

$$p|B_{\text{gcd}(n,m)}.$$

So we may assume m is the maximal divisor n/p.

It follows from (I) that if B_n does *not* have a primitive divisor then

$$B_n \mid 2n \prod_{p|n} B_{\frac{n}{p}}. \qquad (1)$$

Step 2

Take logs in (1):

$$\log B_n \leq \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Step 2

Take logs in (1):

$$\log B_n \leq \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Apply growth rate from (II), $\log B_n \sim hn^2$:

$$hn^2 \leq \log(2n) + hn^2 \sum_{p|n} \frac{1}{p^2}.$$

Step 2

Take logs in (1):

$$\log B_n \leq \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Apply growth rate from (II), $\log B_n \sim hn^2$:

$$hn^2 \leq \log(2n) + hn^2 \sum_{p|n} \frac{1}{p^2}.$$

But $\sum_{p|n} \frac{1}{p^2} < .452\ldots$

Property I

Proof is not trivial and uses p-adic arithmetic.

As motivation run through the argument in the case of the Mersenne sequence.

Lemma For odd primes p, $\text{ord}_p(M_n) > 0$ implies

$$\text{ord}_p(M_{np}) = \text{ord}_p(M_n) + 1.$$

Proof Take p-adic logarithms. Or ...

Lemma For odd primes p, $\text{ord}_p(M_n) > 0$ implies

$$\text{ord}_p(M_{np}) = \text{ord}_p(M_n) + 1.$$

Proof Take p-adic logarithms. Or ...

... let γ denote the order of 2 modulo p. Since $p|M_n$ it follows that $\gamma|n$ so write $n = \gamma k$ for some $k \in \mathbb{N}$. Now the p-adic expansion of 2^γ begins

$$2^\gamma = 1 + c_1 p + c_2 p^2 + \dots$$

Lemma For odd primes p, $\text{ord}_p(M_n) > 0$ implies

$$\text{ord}_p(M_{np}) = \text{ord}_p(M_n) + 1.$$

Proof Take p-adic logarithms. Or ...

... let γ denote the order of 2 modulo p. Since $p|M_n$ it follows that $\gamma|n$ so write $n = \gamma k$ for some $k \in \mathbb{N}$. Now the p-adic expansion of 2^γ begins

$$2^\gamma = 1 + c_1 p + c_2 p^2 + \dots$$

Suppose c_r is the first nonzero coefficient. Then

$$2^{\gamma k} = (1 + c_r p^r + c_{r+1} p^{r+1} \dots)^k.$$

By the binomial theorem $2^{\gamma k} - 1$ is

$$k(c_r p^r + c_{r+1} p^{r+1} \ldots) + \frac{k(k-1)}{2}(c_r p^r + \ldots)^2 \ldots$$

By the binomial theorem $2^{\gamma k} - 1$ is

$$k(c_r p^r + c_{r+1} p^{r+1} \dots) + \frac{k(k-1)}{2}(c_r p^r + \dots)^2 \dots$$

By the ultra-metric inequality the lemma follows because the p-adically largest term is $c_r k p^r$.

Corollary The lemma implies the strong divisibility property of Mersenne numbers:

$$\text{gcd}(M_r, M_s) = M_{\text{gcd}(r,s)}.$$

Let $E_1(\mathbb{Q})$ denote the subgroup of $E(\mathbb{Q})$ whose denominators are divisible by p; in other words, all $Q \in E(\mathbb{Q})$ with

$$|x(Q)|_p > 1.$$

Let $E_1(\mathbb{Q})$ denote the subgroup of $E(\mathbb{Q})$ whose denominators are divisible by p; in other words, all $Q \in E(\mathbb{Q})$ with

$$|x(Q)|_p > 1.$$

The following lemma is the elliptic analogue of the one above for Mersenne numbers.

Lemma If p is odd, for any $O \neq Q \in E_1(\mathbb{Q})$,

$$\mathrm{ord}_p(B_{pQ}) = \mathrm{ord}_p(B_Q) + 1.$$

Proof Take the p-adic elliptic logarithm. Or
...

Proof Take the p-adic elliptic logarithm. Or ...

... assume E has the shape

$$y^2 = x^3 + Ax + B.$$

Let

$$z = x/y, w = 1/y.$$

Dividing the equation through by y^3 and using the substitutions above turns the equation into the following

$$w = z^3 + Azw^2 + Bw^3. \tag{2}$$

Proof Take the p-adic elliptic logarithm. Or ...

... assume E has the shape

$$y^2 = x^3 + Ax + B.$$

Let

$$z = x/y, w = 1/y.$$

Dividing the equation through by y^3 and using the substitutions above turns the equation into the following

$$w = z^3 + Azw^2 + Bw^3. \qquad (2)$$

Call this new curve E'. It too is a group, with identity $[0, 0]$.

Define

$$\phi(x, y) = (z, w) = (x/y, 1/y). \qquad (3)$$

Define

$$\phi(x, y) = (z, w) = (x/y, 1/y). \tag{3}$$

Lemma

The map $\phi : E \to E'$ is a group homomorphism.

For $Q \in E_1(\mathbb{Q}), \phi(Q)$ on E' has z-coordinate divisible by p. On the right hand side of (2) you can keep substituting for w and you obtain a power series with integer coefficients that begins

$$w = z^3 + \cdots \in \mathbb{Z}[[z]].$$

Our assumption that $p|z$ guarantees that the power series for $w = w(z)$ converges p-adically.

Adding points on E'

Two points $P_1 = (z_1, w_1)$ and $P_2 = (z_2, w_2)$ on E' are added in the usual geometric way. The line joining the points is $w = \alpha z + \beta$ where

$$\alpha = \frac{w_1 - w_2}{z_1 - z_2}.$$

Using the power series for the w_i we cancel $z_1 - z_2$.

If $\mathrm{ord}_p(B_{P_1}) = r$ then the corresponding z and w have order r and $3r$ respectively.

If $\mathrm{ord}_p(B_{P_1}) = r$ then the corresponding z and w have order r and $3r$ respectively.

It follows that for $P_1, P_2 \in E_r(\mathbb{Q})$, α as above must be divisible by p^{2r}.

If $\mathrm{ord}_p(B_{P_1}) = r$ then the corresponding z and w have order r and $3r$ respectively.

It follows that for $P_1, P_2 \in E_r(\mathbb{Q})$, α as above must be divisible by p^{2r}.

Also, β must be divisible by p^{3r}.

Substitute equation of the line $w = \alpha z + \beta$ into the equation of the curve to get

$$\alpha z + \beta = z^3 + Az(\alpha z + \beta)^2 + B(\alpha z + \beta)^3.$$

This equation has three roots in z and by the sum of roots formula

$$z_1 + z_2 + z_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + A\alpha^2 + B\alpha^3}.$$

This equation has three roots in z and by the sum of roots formula

$$z_1 + z_2 + z_3 = -\frac{2A\alpha\beta + 3B\alpha^2\beta}{1 + A\alpha^2 + B\alpha^3}.$$

Thus

$$z_1 + z_2 + z_3$$

is divisible by p^{3r}.

Assuming $P_1, P_2 \in E_r(\mathbb{Q})$, the result of doing this is a congruence

$$z(P_1 + P_2) \equiv z(P_1) + z(P_2) \mathrm{mod} p^{3r}. \qquad (4)$$

If $P_1 = P_2$ then taking the tangent instead yields

$$z(2P_1) \equiv 2z(P_1) \mathrm{mod} p^{3r}. \qquad (5)$$

To complete the proof of the lemma apply induction to obtain

$$z(nP) \equiv nz(P) \text{mod} p^{3r}.$$

Property II: An EDS has quadratic exponential growth rate

From the theory of heights,

$$\log \max\{|A_n|, |B_n|^2\} = 2hn^2 + O(1).$$

Property II: An EDS has quadratic exponential growth rate

From the theory of heights,

$$\log \max\{|A_n|, |B_n|^2\} = 2hn^2 + O(1).$$

So the issue is to show that

$$\log |A_n| - 2 \log |B_n|$$

does not grow too quickly. This is achieved by bounding $|x(nP)|$ above suitably.

Property II: An EDS has quadratic exponential growth rate

From the theory of heights,

$$\log \max\{|A_n|, |B_n|^2\} = 2hn^2 + O(1).$$

So the issue is to show that

$$\log |A_n| - 2 \log |B_n|$$

does not grow too quickly. This is achieved by bounding $|x(nP)|$ above suitably.

Use elliptic transcendence theory.

Let z correspond to P under an isomorphism $E(\mathbb{C}) \simeq \mathbb{C}/L$, for some lattice L. Then assume that the x-coordinate of a point is given using the Weierstrass $\wp$-function,

$$x = \wp_L(z) = \frac{1}{z^2} + c_2 z^2 + \dots$$

Write $\{nz\}$ for nz modulo L.

When the quantity $|x(nP)|$ is large it means nz is close to zero modulo L, thus the quantities $|x(nP)|$ and $1/|\{nz\}|^2$ are commensurate.

When the quantity $|x(nP)|$ is large it means nz is close to zero modulo L, thus the quantities $|x(nP)|$ and $1/|\{nz\}|^2$ are commensurate.

On the complex torus, this means the elliptic logarithm is close to zero.

When the quantity $|x(nP)|$ is large it means nz is close to zero modulo L, thus the quantities $|x(nP)|$ and $1/|\{nz\}|^2$ are commensurate.

On the complex torus, this means the elliptic logarithm is close to zero.

So it is sufficient to supply a lower bound for $\{nz\}$ and this can be given by elliptic transcendence theory.

Use David's Theorem from 1995

$$\log |x(nP)| \ll \log n (\log \log n)^3, \qquad (6)$$

where the implied constant depends upon E and the point P.

Use David's Theorem from 1995

$$\log |x(nP)| \ll \log n (\log \log n)^3, \qquad (6)$$

where the implied constant depends upon E and the point P.

Hence

$$\log B_n = hn^2 + O(\log n (\log \log n)^3).$$

Uniformity ‘Proof’

If B_n does *not* have a primitive divisor then

$$\log B_n \leq \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Uniformity 'Proof'

If B_n does *not* have a primitive divisor then

$$\log B_n \leq \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Assume growth rate in the following form,

$$\log B_n = hn^2 + O(\log \Delta_E (\log n)^2)$$

with a uniform constant. Then

$$.548hn^2 \leq \log(2n) + O(\log \Delta_E (\log n)^2).$$

Uniformity 'Proof'

If B_n does *not* have a primitive divisor then

$$\log B_n \le \log(2n) + \sum_{p|n} \log B_{\frac{n}{p}}.$$

Assume growth rate in the following form,

$$\log B_n = hn^2 + O(\log \Delta_E (\log n)^2)$$

with a uniform constant. Then

$$.548hn^2 \le \log(2n) + O(\log \Delta_E (\log n)^2).$$

By Lang's conjecture $\log \Delta_E \ll h$ uniformly so divide through by h to get uniform upper bound for n.

But. . .

In David's Theorem, the dependence of the error term on $\log \Delta_E$ is cubic.

But. . .

In David's Theorem, the dependence of the error term on $\log \Delta_E$ is cubic.

Implied constant is very large.

Therefore expect uniformity results for families of elliptic curves where:

(a) Lang's conjecture is provable and

Therefore expect uniformity results for families of elliptic curves where:

(a) Lang's conjecture is provable and

(b) better transcendence results are possible.

Theorem

[GE+McLaren+Ward JNT 2006]

Let E denote the elliptic curve with equation

$$y^2 = x^3 - T^2 x,$$

where $T \geq 1$ is square-free (guarantees equation is minimal). Suppose $B = (B_n)$ is an EDS coming from $P \in E(\mathbb{Q})$. Then,

Theorem

[GE+McLaren+Ward JNT 2006]

Let E denote the elliptic curve with equation

$$y^2 = x^3 - T^2 x,$$

where $T \geq 1$ is square-free (guarantees equation is minimal). Suppose $B = (B_n)$ is an EDS coming from $P \in E(\mathbb{Q})$. Then,

(i) $x(P) < 0$ implies $Z(B) \leq 10$,

Theorem

[GE+McLaren+Ward JNT 2006]

Let E denote the elliptic curve with equation

$$y^2 = x^3 - T^2 x,$$

where $T \geq 1$ is square-free (guarantees equation is minimal). Suppose $B = (B_n)$ is an EDS coming from $P \in E(\mathbb{Q})$. Then,

(i) $x(P) < 0$ implies $Z(B) \leq 10$,

(ii) $x(P) = \square$ implies $Z(B) \leq 21$.

This result is in line with the classical results stated earlier for Lucas sequences.

This result is in line with the classical results stated earlier for Lucas sequences.

The bound is

This result is in line with the classical results stated earlier for Lucas sequences.

The bound is

(a) uniform

This result is in line with the classical results stated earlier for Lucas sequences.

The bound is

(a) uniform

(b) small.

This result is in line with the classical results stated earlier for Lucas sequences.

The bound is

(a) uniform

(b) small.

However it applies only to a 1-parameter family of elliptic curves.

Note If E is a congruent number curve with positive rank then there are always points with $x(P) < 0$ or $x(P) = \Box$.

Note If E is a congruent number curve with positive rank then there are always points with $x(P) < 0$ or $x(P) = \Box$.

If $x(P) > 0$ then

$$x(P + [0,0]) < 0 \text{ and } x(P + [-T,0]) < 0.$$

Note If E is a congruent number curve with positive rank then there are always points with $x(P) < 0$ or $x(P) = \square$.

If $x(P) > 0$ then

$$x(P + [0,0]) < 0 \text{ and } x(P + [-T,0]) < 0.$$

For any non-torsion P, $x(2P) = \square$.

Example 1

$E : y^2 = x^3 - 25x \;\; P = [-4, 6]$

n	B_n
1	1
2	12
3	2257
4	1494696
5	8914433905
6	178761481355556
7	62419747600438859233
8	53542298628216020922 91248
9	1001926359199672697329083442936609

Note Here you can *see* property (II).

Example 1

n	Factors of B_n
1	1
2	$\underline{2}^2.\underline{3}$
3	$\underline{37}.\underline{61}$
4	$2^3.3.\underline{7}^2.\underline{31}.\underline{41}$
5	$\underline{5}.\underline{13}.\underline{17}.\underline{761}.\underline{10601}$
6	$2^2.3^2.\underline{11}.37.61.\underline{71}.\underline{587}.\underline{4799}$
7	$\underline{197}.\underline{421}.\underline{215153}.\underline{3498052153}$
8	$2^4.3.7^2.31.41.\underline{113279}.\underline{3344161}.\underline{4728001}$
9	$37.61.\underline{26209}.\underline{14764833973}.\underline{114716324740014 1}$

Note Here you can *see* property (I).

Example 2

$E : y^2 = x^3 - 36x \;\; P = [-3, 9]$

n	Factors of B_n
1	1
2	$\underline{2}$
3	$\underline{37}$
4	$2^2.\underline{5}.\underline{7}$
5	$\underline{13}.\underline{3121}$
6	$2.3.\underline{11}.\underline{23}.37.\underline{47}$
7	$\underline{14281}.\underline{140449}$
8	$2^3.5.7.\underline{1151}.\underline{1201}.\underline{1249}$
9	$37.\underline{2148661}.\underline{31904497}$
10	$2.13.\underline{17}.\underline{19}.\underline{73}.\underline{97}.\underline{139}.\underline{239}.\underline{719}.3121$

:

Example 3

$E : y^2 = x^3 - 49x \;\; P = [25, 120]$

n	Factors of B_n
1	1
$\underline{2}$	$\underline{2}^3.\underline{3}.\underline{5}$
3	$\underline{263}.\underline{937}$
4	$2^4.3.5.\underline{113}.\underline{337}.\underline{463}$
5	$\underline{17}.\underline{89}.\underline{313}.\underline{6481}.\underline{111119}$
6	$2^3.3^2.5.\underline{11}.\underline{23}.\underline{131}.\underline{167}.263.\underline{673}.937.\underline{141793}$
7	$\underline{7}.\underline{5039}.\underline{7673}.\underline{40993}.\underline{224558153}.\underline{9347641241}$
8	

Question

What is the true Zsigmondy bound for the congruent number curves?

Theorem [Ingram JNT to appear]

For square-free $T \geq 1$, let E denote the elliptic curve with equation

$$y^2 = x^3 - T^2 x.$$

Suppose $B = (B_n)$ is an EDS coming from $P \in E(\mathbb{Q})$. If $x(P) < 0$ or $x(P) = \square$ then $Z(B) \leq 2$.

How?

How?

Ingram reduces the cases left untouched by our theorem to a finite set of solvable Thue equations.

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

n even: $\log B_n > .75hn^2 - c_1 \log T$

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

n even: $\log B_n > .75hn^2 - c_1 \log T$

n odd $x(P) < 0$: $\log B_n > hn^2 - c_2 \log T$

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

n even: $\log B_n > .75hn^2 - c_1 \log T$

n odd $x(P) < 0$: $\log B_n > hn^2 - c_2 \log T$

n odd $x(P) = \square$: $\log B_n > .25hn^2 - c_3 \log T$

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

n even: $\log B_n > .75hn^2 - c_1 \log T$

n odd $x(P) < 0$: $\log B_n > hn^2 - c_2 \log T$

n odd $x(P) = \square$: $\log B_n > .25hn^2 - c_3 \log T$

Fluke here: $\sum_{2 \nmid p} 1/p^2 < .25$

EMW paper - main ideas

Use a lower bound for $\log B_n$ which is weaker in n but stronger in $\log T$.

n even: $\log B_n > .75hn^2 - c_1 \log T$

n odd $x(P) < 0$: $\log B_n > hn^2 - c_2 \log T$

n odd $x(P) = \square$: $\log B_n > .25hn^2 - c_3 \log T$

Fluke here: $\sum_{2\nmid p} 1/p^2 < .25$

Strong form of Lang's conjecture (Bremner, Silverman + Tzanakis):

$$h > .5 \log T$$

Curves in homogeneous form

Suppose E denotes an elliptic curve defined by an equation

$$E_D : X^3 + Y^3 = D,$$

for some non-zero, cube-free $D \in \mathbb{Q}$. Let P denote a $\mathbb{Q}$-rational point. Write, in lowest terms

$$P = \left(\frac{A_P}{B_P}, \frac{C_P}{B_P}\right) \text{ and } nP = \left(\frac{A_n}{B_n}, \frac{C_n}{B_n}\right).$$

Theorem[GE+Stevens+Phuksuwan] Provided $D \in \mathbb{Q}$ is cube-free, $Z(B) \leq 42$.

Theorem[GE+Stevens+Phuksuwan] Provided $D \in \mathbb{Q}$ is cube-free, $Z(B) \leq 42$.

Improvements are almost certainly possible.

Proof - main ideas

Use the bi-rational transformation between the homogeneous curve E_D, and the curve in Weierstrass form

$$E'_D : y^2 = x^3 - 432D^2.$$

Proof - main ideas

Use the bi-rational transformation between the homogeneous curve E_D, and the curve in Weierstrass form

$$E'_D : y^2 = x^3 - 432D^2.$$

The map is given by

$$X = \frac{36D + y}{6x} \text{ and } Y = \frac{36D - y}{6x}.$$

If $P' \in E'_D(\mathbb{Q})$ corresponds to $P \in E_D(\mathbb{Q})$ under the transformation, write

$$nP' = \left(\frac{A'_n}{B'^2_n}, \frac{C'_n}{B'^3_n} \right).$$

Then

$$X(nP) = \frac{36DB'^3_n + C'_n}{6A'_nB'_n}.$$

Both A_n' and B_n' have primitive divisors from some point.

Both A'_n and B'_n have primitive divisors from some point.

We can prove a uniform Zsigmondy bound $Z(A')$ for $A' \ldots$

Both A'_n and B'_n have primitive divisors from some point.

We can prove a uniform Zsigmondy bound $Z(A')$ for $A' \ldots$

... but we cannot prove a uniform Zsigmondy bound for B').

Both A'_n and B'_n have primitive divisors from some point.

We can prove a uniform Zsigmondy bound $Z(A')$ for $A' \ldots$

... but we cannot prove a uniform Zsigmondy bound for B').

Use Jedrzejak's explicit version of Lang's conjecture for this curve.

2 PRIMALITY

Examples

1. (Chudnovsky and Chudnovsky 1986)

$$E: \quad y^2 = x^3 + 26, \quad P = [-1, 5]$$

The term B_{29} is a prime with 286 decimal digits.

$$E: \quad y^2 = x^3 + 15, \quad P = [1, 4]$$

The term B_{41} is a prime with 510 decimal digits.

Examples

1. (Chudnovsky and Chudnovsky 1986)

$$E: \quad y^2 = x^3 + 26, \quad P = [-1, 5]$$

The term B_{29} is a prime with 286 decimal digits.

$$E: \quad y^2 = x^3 + 15, \quad P = [1, 4]$$

The term B_{41} is a prime with 510 decimal digits.

They let n run out to 100.

2. (Bríd Ní Fhlathuín 1999)

$$E: \quad y^2 + y = x^3 - x, \quad P = [0, 0]. \qquad (7)$$

The term B_{409} is a prime with 1857 decimal digits.

2. (Bríd Ní Fhlathuín 1999)

$$E: \quad y^2 + y = x^3 - x, \quad P = [0, 0]. \tag{7}$$

The term B_{409} is a prime with 1857 decimal digits.

3. (GE 2006)

Same sequence as in (7). The term B_{1291} is a prime with 18498 decimal digits.

These large primes are technically *pseudo-primes* to 20 bases in the sense of the Miller-Rabin test. Thus the probability they are composite is less than

$$\frac{1}{4^{20}} < .0000000000001$$

These large primes are technically *pseudo-primes* to 20 bases in the sense of the Miller-Rabin test. Thus the probability they are composite is less than

$$\frac{1}{4^{20}} < .000000000001$$

It takes PARI-GP just under 10 hours to check B_{1291} on a PC. It takes MAGMA about 2 hours.

Further Calculations

In 1999, GE+Einsielder+Ward let n run out to 500 in the Chudnovsky's calculations. No further prime terms appeared.

Further Calculations

In 1999, GE+Einsielder+Ward let n run out to 500 in the Chudnovsky's calculations. No further prime terms appeared.

Example (7) has only produced 14 prime terms in total.

Conjecture

Only finitely many terms of an elliptic divisibility sequence are primes. If the curve is given in minimal form, the number of prime terms is uniformly bounded.

Conjecture
Only finitely many terms of an elliptic divisibility sequence are primes. If the curve is given in minimal form, the number of prime terms is uniformly bounded.

Note Uniformly bounded means independent of curve and point. Perhaps the bound is 32 - see later.

The Curve $y^2 + y = x^3 - x$.

n	digits of B_n
5	1
7	1
8	1
9	1
11	2
12	2
13	2
19	4
23	6
29	10
83	77
101	114
409	1857
1291	18498

Heuristic Arguments

1. Lenstra and Wagstaff on Mersenne

By the PNT, the probability that $N > 1$ is prime is $1/\log N$.

Heuristic Arguments

1. Lenstra and Wagstaff on Mersenne

By the PNT, the probability that $N > 1$ is prime is $1/\log N$.

Does this suggest that the number of Mersenne primes M_n with $n < X$ is roughly

$$\sum_{n<X} \frac{1}{\log M_n} \sim \frac{\log X}{\log 2}? \tag{8}$$

The formula in (8) does not match the evidence.

The formula in (8) does not match the evidence.

Lenstra and Wagstaff refined this to argue that the number of Mersenne primes M_n with $n < X$ is asymptotically

$$c \log X$$

where

$$c = e^{\gamma} / \log 2.$$

In other words, PNT gives the asymptotic growth rate. Refinement using congruence arguments gives leading constant.

2. Application to EDSs

Arguing along the same lines suggests that the number of prime terms B_n having $n < X$ is roughly

$$\sum_{n<X} \frac{1}{\log B_n}. \tag{9}$$

2. Application to EDSs

Arguing along the same lines suggests that the number of prime terms B_n having $n < X$ is roughly

$$\sum_{n<X} \frac{1}{\log B_n}. \tag{9}$$

Growth rate shows this sum is bounded by

$$\frac{1}{h} \sum_{n<X} \frac{1}{n^2} < \frac{\pi^2}{6h}.$$

2. Application to EDSs

Arguing along the same lines suggests that the number of prime terms B_n having $n < X$ is roughly

$$\sum_{n<X} \frac{1}{\log B_n}. \tag{9}$$

Growth rate shows this sum is bounded by

$$\frac{1}{h} \sum_{n<X} \frac{1}{n^2} < \frac{\pi^2}{6h}.$$

Now $h > 0$ is known to be uniformly bounded below. Hence the sum in (9) is uniformly bounded above.

The heuristic argument suggested that if $h > 0$ is small then we might get more primes for our money. . .

Example 4
Let P denote the point $[-386, -3767]$ on the elliptic curve

$$y^2 + xy = x^3 - 141875x + 13893057.$$

Example 4

Let P denote the point $[-386, -3767]$ on the elliptic curve

$$y^2 + xy = x^3 - 141875x + 13893057.$$

The EDS has B_n equal to a prime for at least 32 values of n. The largest known is B_{1811} which has 6438 decimal digits.

Noam Elkies keeps a web site with a table of small height rational points:

www.math.harvard.edu/$\sim$ elkies/low_height.html

Higher rank

Example

The curve

$$y^2 = x^3 - 28x + 52$$

has rank 2, with generators $P_1 = (-2, 10)$ and $P_2 = (-4, 10)$. It seems likely that there are *infinitely* many pairs $n_1,\ n_2 \in \mathbb{Z}$ for which

$$x(n_1 P_1 + n_2 P_2)$$

has a prime square denominator.

Possibly there are asymptotically

$$\rho \log T$$

such values with $\max\{|n_1|, |n_2|\} < T$, where $\rho > 0$ is a constant depending upon P_1, P_2 and E.

Heuristic Argument

Using transcendence theory as before, the logarithm of the denominator of

$$x(n_1P_1 + n_2P_2)$$

is roughly $Q(\underline{n})$, some positive definite quadratic form.

Expected number of pairs $\underline{n} = (n_1, n_2) \in \mathbb{Z}^2$ with $|\underline{n}| < X$ for which

$$x(n_1 P_1 + n_2 P_2)$$

has a prime square denominator is

$$\sum_{0<|\underline{n}|<X} \frac{1}{Q(\underline{n})}.$$

The sum is approximately

$$\int_{1 \leq |\underline{x}| < X} \frac{\mathrm{d}\underline{x}}{Q(\underline{x})}.$$

The sum is approximately

$$\int_{1 \le |\underline{x}| < X} \frac{\mathrm{d}\underline{x}}{Q(\underline{x})}.$$

Changing the variables shows this is roughly

$$\frac{2\pi}{R} \int_1^X \frac{\mathrm{d}t}{t} \sim \frac{2\pi}{R} \log X$$

where R is the determinant of the form - the regulator of the two points P_1, P_2.

Computations suggest you get roughly $\rho \log X$ primes but the constant is not the one predicted by the heuristic argument (as per Mersenne).

Question

Do you get a greater frequency of prime terms if the regulator is small?

Prime Frequency $|\underline{x}| < 100$

Curve	Generators	Primes	Regulator
[0,0,1,-199,1092]	[-13,38],[-6,45]	264	0.0360
[0,0,1,-27,56]	[-3,10],[0,7]	209	0.0803
[0,0,0,-28,52]	[-4,10],[-2,10]	200	0.0813
[1,-1,0,-10,16]	[-2,6],[0,4]	190	0.0878
[1,-1,1,-42,105]	[17,-73],[-5,15]	182	0.0887

Prime Frequency $|\underline{x}| < 100$

Curve	Generators	Primes	Regulator
[0,0,1,-199,1092]	[-13,38],[-6,45]	264	0.0360
[0,0,1,-27,56]	[-3,10],[0,7]	209	0.0803
[0,0,0,-28,52]	[-4,10],[-2,10]	200	0.0813
[1,-1,0,-10,16]	[-2,6],[0,4]	190	0.0878
[1,-1,1,-42,105]	[17,-73],[-5,15]	182	0.0887

Taken from a larger table made by Peter Rogers

http://www.mth.uea.ac.uk/~h090/2deds.htm

Prime Frequency $|\underline{x}| < 100$

Curve	Generators	Primes	Regulator
[1,1,0,-29,61]	[-6,11],[-1,10]	155	0.1482
[1,0,1,-3,2]	[0,1],[1,0]	138	0.1490
[0,1,0,-5,4]	[-1,3],[0,2]	167	0.1502
[0,1,1,-2,0]	[0,0],[1,0]	165	0.1525
[1,0,1,-12,14]	[12,-47],[-1,5]	143	0.1578